

Secure Wireless Information and Power Transfer in Large-Scale MIMO Relaying Systems with Imperfect CSI

Xiaoming Chen^{†,‡}, Jian Chen[†], and Tao Liu[†]

[†] College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, China.

[‡] National Mobile Communications Research Laboratory, Southeast University, China.

Email: {chenxiaoming, chenjian04, tliu}@nuaa.edu.cn

Abstract—In this paper, we address the problem of secure wireless information and power transfer in a large-scale multiple-input multiple-output (LS-MIMO) amplify-and-forward (AF) relaying system. The advantage of LS-MIMO relay is exploited to enhance wireless security, transmission rate and energy efficiency. In particular, the challenging issues incurred by short interception distance and long transfer distance are well addressed simultaneously. Under very practical assumptions, i.e., no eavesdropper's channel state information (CSI) and imperfect legitimate channel CSI, this paper investigates the impact of imperfect CSI, and obtains an explicit expression of the secrecy outage capacity in terms of transmit power and channel condition. Then, we propose an optimal power splitting scheme at the relay to maximize the secrecy outage capacity. Finally, our theoretical claims are validated by simulation results.

I. INTRODUCTION

Energy harvesting facilitates the battery charging to prolong the lifetime of wireless networks, especially under some extreme conditions, such as battle-field, underwater and body area networks [1]. Wherein, electromagnetic wave based wireless power transfer has received considerable research attentions from academic and industry due to two-fold reasons. First, it is a controllable power transfer mode. Second, information and power can be simultaneously transferred in the form of electromagnetic wave [2] [3].

Similar to information transmission, wireless power transfer may suffer from channel fading, resulting in low energy efficiency. In this end, energy beamforming is proposed by deploying multiple antennas at the power source [4] [5]. The impact of channel state information (CSI) at the power source on the performance of wireless information and power transfer (WIPT) is quantitatively analyzed in [6]. Recently, large scale multiple input multiple output (LS-MIMO) techniques are also introduced to significantly improve the efficiency of WIPT by exploiting the high spatial resolution [7]. Moreover, relaying technique is also proved as an effective way of improving

the performance of WIPT by shortening the transfer distance, since the distance has a great impact on both information and power transfer [8]. A two-way relaying scheme is proposed in [9] to offer a higher transmission rate with the harvested energy. In fact, through combining relaying schemes and multi-antenna techniques, especially the LS-MIMO techniques, the performance of WIPT can be improved significantly, even in the case of long-distance transfer. However, to the best of our knowledge, there is no work studying the problem of the LS-MIMO relaying techniques for WIPT.

Meanwhile, information transfer may encounter interception from the eavesdropper due to the broadcast nature of wireless channels. In recent years, as a supplementary of encryption techniques, physical layer security is used to realize secure communications, by exploiting wireless channel characteristics, i.e., fading and noise. The performance of physical layer security is determined by the performance difference between the legitimate and eavesdropper channels [10]. Thus, the LS-MIMO relaying technique is also an effective way of improving the secrecy performance [11]. For secure WIPT, long-distance transfer and short-distance interception are two challenging issues [12] [13]. To solve them, we introduce the amplify-and-forward (AF) LS-MIMO relaying technique into secure WIPT. The contributions of this paper are two-fold:

- 1) We derive an explicit expression of the secrecy outage capacity for such a secure WIPT system in terms of transmit power, CSI accuracy and transfer distance.
- 2) We propose a power splitting scheme at the relay, so as to maximize the secrecy outage capacity.

The rest of this paper is organized as follows. We first give an overview of the secure WIPT system based on the LS-MIMO AF relaying scheme in Section II, and then derive the secrecy outage capacity under imperfect CSI in Section III. In Section IV, we present some simulation results to validate the effectiveness of the proposed scheme. Finally, we conclude the whole paper in Section V.

II. SYSTEM MODEL

We consider a time division duplex (TDD) LS-MIMO AF relaying system, where a single antenna source communicates

This work was supported by the National Natural Science Foundation of China (No. 61301102), the Natural Science Foundation of Jiangsu Province (No. BK20130820), the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2012D16), the Doctoral Fund of Ministry of Education of China (No. 20123218120022) and the China Postdoctoral Science Foundation Funded Project (No. 2014T70517).

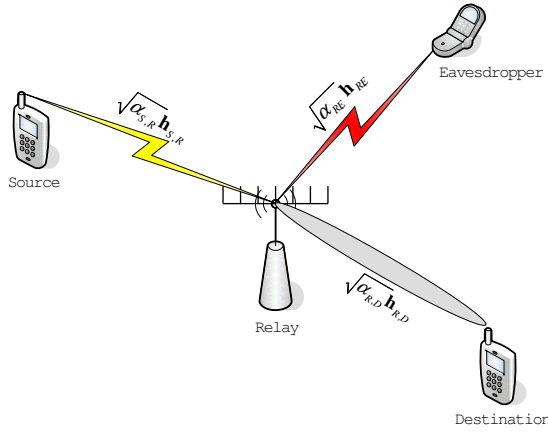


Fig. 1. An overview of the secure WIPT relaying system.

with a single antenna destination aided by a multi-antenna relay, while a single antenna passive eavesdropper intends to intercept the message, as shown in Fig.1. Note that the number of antenna at the relay N_R is quite large for such an LS-MIMO relaying system, i.e., $N_R = 100$ or greater. The relay only has limited energy to maintain the active state, so it needs to harvest enough energy from the source for information transmission. Considering the limited storage, the relay should be charged from the source slot by slot.

The whole system is operated in slotted time of length T , and the relay works in the half-duplex mode. Then, the information transmission from the source to the destination via the aid of the relay requires two time slots. Specifically, in the first time slot, the source sends the signal, and the relay splits the received signal into two streams, one for energy harvesting and the other for information processing. During the second time slot, the relay forwards the post-processing signal to the destination with the harvested energy. Note that the direct link from the source to the destination is unavailable due to a long distance. We assume that the eavesdropper is far away from the source and is close to the relay, since it thought the signal comes from the relay. Note that it is a common assumption in related literature [11] [14], since it is difficult for the eavesdropper to overhear the signals from the source and the relay simultaneously. Then, the eavesdropper only monitors the transmission from the relay to the destination.

We use $\sqrt{\alpha_{i,j}}\mathbf{h}_{i,j}$ to denote the channel from i to j , where $i \in \{S, R\}$ and $j \in \{R, D, E\}$ with S, R, D, E representing the source, the relay, the destination and the eavesdropper, respectively. $\alpha_{i,j}$ is the distance-dependent path loss and $\mathbf{h}_{i,j}$ is the small scale fading. In this paper, we model $\mathbf{h}_{i,j}$ as Gaussian distribution with zero mean and unit variance. $\alpha_{i,j}$ remains constant during a relatively long period and $\mathbf{h}_{i,j}$ fades independently slot by slot. Thus, the received signal at the relay in the first time slot can be expressed as

$$\mathbf{y}_R = \sqrt{P_S \alpha_{S,R}} \mathbf{h}_{S,R} s + \mathbf{n}_R, \quad (1)$$

where s is the normalized Gaussian distributed transmit signal, P_S is the transmit power at the source, and \mathbf{n}_R is the additive

Gaussian white noise with zero mean and unit variance at the relay. As mentioned above, the relay splits the received signal \mathbf{y}_R into energy harvesting stream with proportional factor θ and signal processing stream with $1 - \theta$. Then, according to the law of energy conservation, the harvesting energy at the relay is given by

$$E_h = \theta \eta \alpha_{S,R} P_S \|\mathbf{h}_{S,R}\|^2 T, \quad (2)$$

where the constant parameter η , scaling from 0 to 1, is the efficiency ratio at the relay for converting the harvested energy to the electrical energy to be stored [5] [6]. With the harvested energy, the relay forwards the post-processing signal \mathbf{r} to the destination. Then the received signals at the destination and the eavesdropper are given by

$$y_D = \sqrt{\alpha_{R,D}} \mathbf{h}_{R,D}^H \mathbf{r} + n_D, \quad (3)$$

and

$$y_E = \sqrt{\alpha_{R,E}} \mathbf{h}_{R,E}^H \mathbf{r} + n_E, \quad (4)$$

respectively, where n_D and n_E are the additive Gaussian white noises with zero mean and unit variance at the destination and the eavesdropper. $\mathbf{r} = \sqrt{1 - \theta} \mathbf{W} \mathbf{y}_R$ is the post-processing signal with \mathbf{W} being a transform matrix.

We assume the relay has full CSI $\mathbf{h}_{S,R}$ by channel estimation, and gets partial CSI $\hat{\mathbf{h}}_{R,D}$ via channel reciprocity in TDD systems. Due to duplex delay between uplink and downlink, there is a certain degree of mismatch between the estimated CSI $\hat{\mathbf{h}}_{R,D}$ and the real CSI $\mathbf{h}_{R,D}$, whose relation can be expressed as [15]

$$\mathbf{h}_{R,D} = \sqrt{\rho} \hat{\mathbf{h}}_{R,D} + \sqrt{1 - \rho} \mathbf{e}, \quad (5)$$

where \mathbf{e} is the error noise vector with independent and identically distributed (i.i.d.) zero mean and unit variance complex Gaussian entries. ρ , scaling from 0 to 1, is the correlation coefficient between $\hat{\mathbf{h}}_{R,D}$ and $\mathbf{h}_{R,D}$. A larger ρ means better CSI accuracy. If $\rho = 1$, the relay has full CSI $\mathbf{h}_{R,D}$. Additionally, due to the hidden property of the eavesdropper, the CSI $\mathbf{h}_{R,E}$ is unavailable. Therefore, \mathbf{W} is designed only based on $\mathbf{h}_{S,R}$ and $\hat{\mathbf{h}}_{R,D}$, but is independent of $\mathbf{h}_{R,E}$. Considering the better performance of maximum ratio combination (MRC) and maximum ratio transmission (MRT) in LS-MIMO systems, we design \mathbf{W} by combining MRC and MRT. Mathematically, the transform matrix is given by

$$\mathbf{W} = \kappa \frac{\hat{\mathbf{h}}_{R,D} \mathbf{h}_{S,R}^H}{\|\hat{\mathbf{h}}_{R,D}\| \|\mathbf{h}_{S,R}\|}, \quad (6)$$

where κ is the power constraint factor. To fulfill the energy constraint at the relay, κ can be computed as

$$\kappa^2 ((1 - \theta) P_S \alpha_{S,R} \|\mathbf{h}_{S,R}\|^2 + 1) T = \theta \eta \alpha_{S,R} P_S \|\mathbf{h}_{S,R}\|^2 T. \quad (7)$$

Based on the AF relaying scheme, the signal-to-noise ratio (SNR) at the destination is given by (8) at the top of the next page, where $a = \eta P_S^2 \alpha_{S,R}^2 \alpha_{R,D}$, $b = \eta P_S \alpha_{S,R} \alpha_{R,D}$ and $c = P_S \alpha_{S,R}$. Similarly, the received SNR at the eavesdropper is given by (9) at the top of this page, where $e = \eta P_S^2 \alpha_{S,R}^2 \alpha_{R,E}$ and $f = \eta P_S \alpha_{S,R} \alpha_{R,E}$.

$$\begin{aligned}\gamma_D &= \frac{|\sqrt{\alpha_{R,D}} \mathbf{h}_{R,D}^H \sqrt{1-\theta} \mathbf{W} \sqrt{P_S \alpha_{S,R}} \mathbf{h}_{S,R}|^2}{\|\sqrt{\alpha_{R,D}} \mathbf{h}_{R,D}^H \mathbf{W}\|^2 + 1} \\ &= \frac{a\theta(1-\theta) |\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^4}{b\theta |\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1)},\end{aligned}\quad (8)$$

$$\gamma_E = \frac{e\theta(1-\theta) |\mathbf{h}_{R,E}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^4}{f\theta |\mathbf{h}_{R,E}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1)},\quad (9)$$

Letting C_D and C_E be the legitimate channel and the eavesdropper channel capacities, then the secrecy rate is given by $C_{SEC} = [C_D - C_E]^+$, where $[x]^+ = \max(x, 0)$ [10]. Since there is no knowledge of the eavesdropper channel at the source and relay, it is impossible to maintain a steady secrecy rate over all realizations of fading channels. In this context, we take the secrecy outage capacity C_{SOC} as the performance metric, which is defined as the maximum available rate while the outage probability that the transmission rate surpasses the secrecy rate is equal to a given value ε , namely

$$P_r(C_{SOC} > C_D - C_E) = \varepsilon. \quad (10)$$

III. OPTIMAL POWER SPLITTING

In this section, we first analyze the secrecy outage capacity of such an LS-MIMO AF relaying system with energy harvesting, and then derive an optimal power splitting scheme to determine the proportional factor θ .

A. Secrecy Outage Capacity

According to (10), the secrecy outage capacity is jointly determined by the legitimate and eavesdropper channel capacities, so we first analyze the legitimate channel capacity. Based on the received SNR at the destination in (8), we have the following theorem:

Theorem 1: The legitimate channel capacity in an LS-MIMO AF relaying system under imperfect CSI can be approximated as $C_D = W \log_2 \left(1 + \frac{a\theta(1-\theta)\rho N_R^3}{b\theta \rho N_R^2 + c(1-\theta)N_R + 1} \right)$, where W is a half of the spectral bandwidth.

Proof: Please refer to Appendix I. ■

It is found that the legitimate channel capacity is a constant due to channel hardening in such an LS-MIMO AF relaying system. Then, according to the definition of the secrecy outage capacity, we have a theorem as below:

Theorem 2: Given an outage probability bound by ε , the secrecy outage capacity for an LS-MIMO AF relaying scheme is $C_{SOC} = W \log_2 \left(1 + \frac{a\theta(1-\theta)\rho N_R^3}{b\theta \rho N_R^2 + c(1-\theta)N_R + 1} \right) - W \log_2 \left(1 + \frac{e\theta(1-\theta)N_R^2 \ln \varepsilon}{f\theta N_R \ln \varepsilon - c(1-\theta)N_R - 1} \right)$.

Proof: Please refer to Appendix II. ■

While Theorem 2 is useful to study the secure wireless information and power transfer system's secrecy outage capacity, the expression is in general too complex to gain insight. Motivated by this, we carry out asymptotic analysis on the

secrecy outage capacity at high transmit power regime, and derive the following theorem:

Theorem 3: At high transmit power regime, the secrecy outage capacity in this case is independent of transmit power P_S . There exists a performance upper bound on the secrecy outage capacity.

Proof: Please refer to Appendix III. ■

Remarks: The secrecy outage capacity will be saturated once the transmit power surpasses a threshold. This is because the AF relaying system is noise limited due to noise amplification at the relay in this case. Thus, it makes sense to find the minimum power that achieves the maximum secrecy outage capacity.

B. Optimal Power Splitting

According to Theorem 2, for a given transmit power, the secrecy outage capacity is a function of power splitting ratio θ . Intuitively, a large θ leads to a high transmit power at the relay, but the received signal power decreases. Moreover, from the view of wireless security, a high transmit power at the relay may also increase the interception probability. Thus, it is necessary to optimize the power splitting ratio, so as to maximize the secrecy outage capacity.

Since $\log_2(x)$ is an increasing function, in order to maximize the secrecy outage capacity, it is equivalent to maximizing the term $\frac{1 + \frac{a\theta(1-\theta)\rho N_R^3}{b\theta \rho N_R^2 + c(1-\theta)N_R + 1}}{1 + \frac{e\theta(1-\theta)N_R^2 \ln \varepsilon}{f\theta N_R \ln \varepsilon - c(1-\theta)N_R - 1}}$. Thus, the optimal power splitting can be described as the following optimization problem:

$$\begin{aligned}\text{OP1 : } & \max_{\theta} \frac{1 + \frac{a\theta(1-\theta)\rho N_R^3}{b\theta \rho N_R^2 + c(1-\theta)N_R + 1}}{1 + \frac{e\theta(1-\theta)N_R^2 \ln \varepsilon}{f\theta N_R \ln \varepsilon - c(1-\theta)N_R - 1}} \\ & \text{s.t. } 0 \leq \theta \leq 1.\end{aligned}\quad (11)$$

The objective function is not concave, so it is difficult to provide a closed-form expression for the optimal θ . However, because (11) is a one-dimensional function of θ , it is possible to get the optimal θ by numerical searching. Specifically, by scaling θ from 0 to 1 with a fixed step, the optimal θ related to the maximum objective function is obtained.

IV. NUMERICAL RESULTS

To examine the accuracy and effectiveness of the derived theoretical results for secure WIPT in an LS-MIMO AF

relaying system, we present several simulation results in the following scenarios: we set $N_R = 100$, $W = 10\text{KHz}$, $\eta = 0.8$, $\theta = 0.1$ and $\rho = 0.9$ without extra explanation. The relay is in the middle of a line between the source and the destination. We normalize the path loss as $\alpha_{S,R} = \alpha_{R,D} = 1$, and use $\alpha_{R,E}$ to denote the relative interception path loss. Specifically, if $\alpha_{R,E} > 1$, the interception distance is shorter than the legitimate propagation distance, and then the interception becomes strong. In addition, we use $\text{SNR} = 10 \log_{10} P_S$ to represent the transmit signal-to-noise ratio (SNR) in dB at the source.

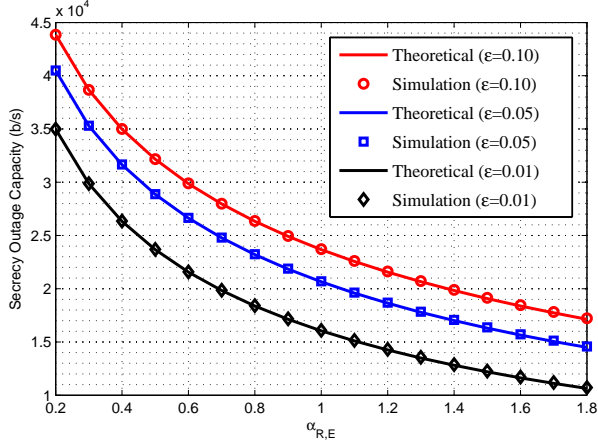


Fig. 2. Comparison of theoretical and simulation results with different $\alpha_{R,E}$.

First, we validate the accuracy of the theoretical results with $\text{SNR}=10\text{dB}$. As shown in Fig.2, the theoretical results coincide with the simulations nicely in the whole $\alpha_{R,E}$ region under different requirements of outage probability. Given a outage probability bound by ε , as $\alpha_{R,E}$ increases, the secrecy outage capacity decreases gradually. This is because the interception capacity of the eavesdropper enhances due to the shorter interception distance. On the other hand, for a given $\alpha_{R,E}$, the secrecy outage capacity improves with the increase of ε , since the secrecy outage capacity is an increasing function of outage probability.

Second, we investigate the impact of power transfer distance on the secrecy outage capacity with $\alpha_{R,E} = 1$, $\varepsilon = 0.01$ and $\text{SNR}=0\text{dB}$ for secure SWIP. Note that optimal power splitting is adopted to improve the secrecy outage capacity. As seen in Fig.3, even at a small $\alpha_{S,R}$, namely long transfer distance, there is a large secrecy outage capacity. As a simple example, at $\alpha_{S,R} = 0.2$, the proposed scheme with $N_r = 100$ can achieve $C_{SOC}^{AF} = 24 \text{ Kb/s}$. As N_r increases, the secrecy outage capacity significantly improves. Thus, the proposed scheme can solve the challenging problem of long-distance transfer for secure WIPT.

Then, we examine the effect of interception distance on the secrecy outage capacity with $\varepsilon = 0.01$ and $\text{SNR}=0\text{dB}$ for secure SWIP. Similarly, optimal power splitting is adopted to improve the secrecy outage capacity. As seen in Fig.4, even at a large $\alpha_{R,E}$, namely short interception distance,

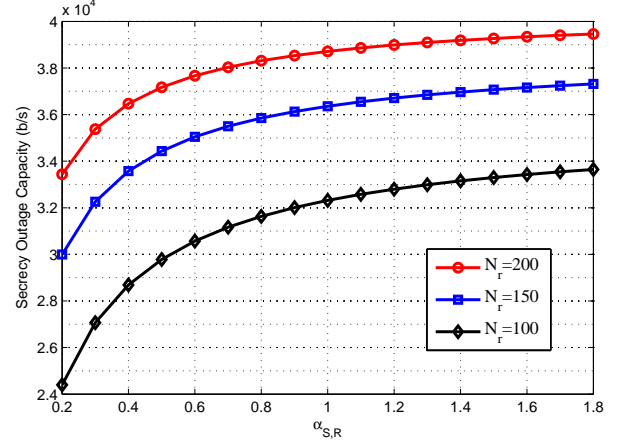


Fig. 3. Performance comparison with different $\alpha_{S,R}$.

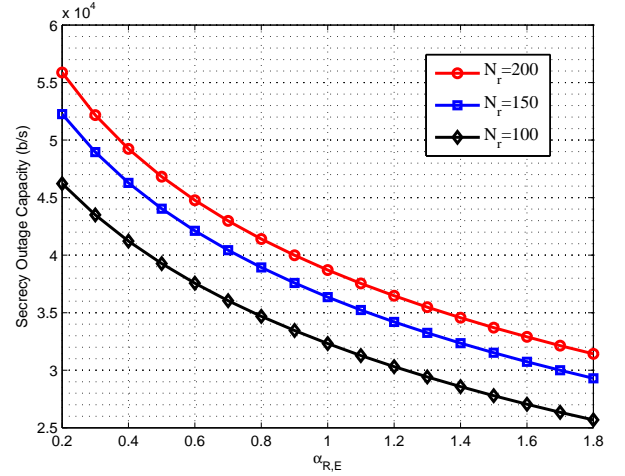


Fig. 4. Performance comparison with different $\alpha_{R,E}$.

there is a large secrecy outage capacity. As a simple example, at $\alpha_{R,E} = 1.8$, the proposed scheme with $N_r = 100$ can achieve $C_{SOC}^{AF} = 25 \text{ Kb/s}$. As N_r increases, the secrecy outage capacity significantly improves. Thus, the proposed scheme can solve the challenging problem of short-distance interception for secure WIPT.

Next, we show the impact of SNR on the secrecy outage capacity with $\alpha_{R,E} = 1$. As seen in Fig.5, the secrecy outage capacity is an increasing function of SNR. However, as SNR increases, the secrecy outage capacity will be saturated. This is because the AF relaying system is noise limited due to noise amplification, which confirmed the claim in Theorem 3. Thus, it makes sense to find the optimal SNR to maximize the secrecy outage capacity in LS-MIMO relaying systems with the minimum transmit power.

Finally, we check the effectiveness of the proposed optimal power splitting scheme with respect to a fixed scheme. Specifically, the fixed scheme sets θ as 0.1 fixedly regardless of channel condition and transmit power. As seen in Fig.6, the proposed scheme performs better obviously. Especially, as

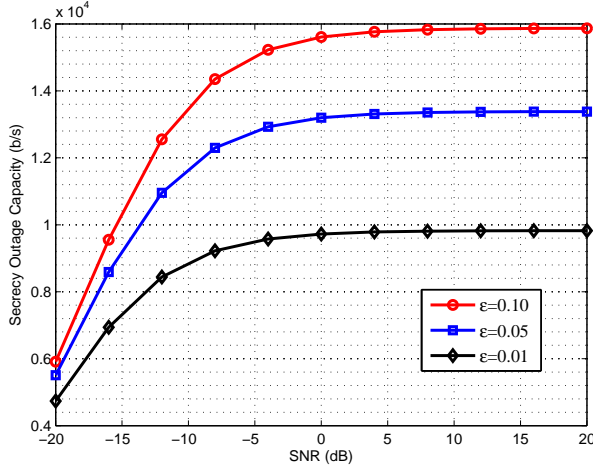


Fig. 5. Performance comparison with different SNRs.

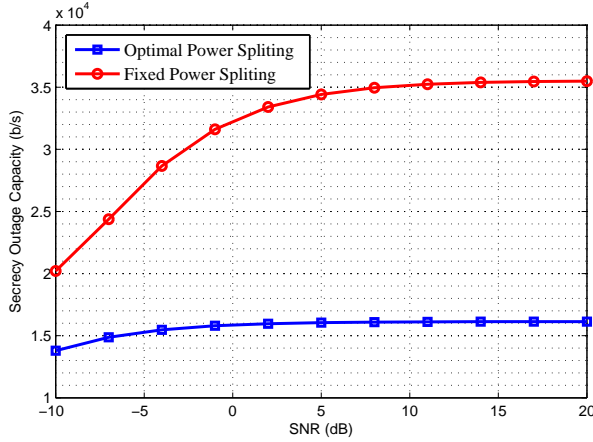


Fig. 6. Performance comparison with different power splitting schemes.

SNR increases, the performance gain becomes larger. Note that the proposed scheme also will suffer from performance saturation. However, the performance bound can be lifted by adding antennas at the relay, which is a main advantage of the LS-MIMO relaying scheme for secure WIPT.

V. CONCLUSION

A major contribution of this paper is the introduction of the LS-MIMO relaying technique into secure wireless information and power transfer to significantly enhance wireless security and improve transmission rate. This paper derives a closed-form expression of the secrecy outage capacity in terms of transmit SNR, power splitting ratio, antenna number and interception distance. Furthermore, through maximizing the secrecy outage capacity, we present a power splitting scheme, which has a huge performance gain with respect to the fixed scheme.

APPENDIX A PROOF OF THEOREM 1

Based on the SNR γ_D at the destination, the legitimated channel capacity can be expressed as

$$\begin{aligned}
 C_D &= W \log_2 \left(1 + a\theta(1-\theta) \|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}\|^2 \|\mathbf{h}_{S,R}\|^4 \right. \\
 &\quad \left. \Big/ \left(b\theta \|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}\|^2 \|\mathbf{h}_{S,R}\|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1) \right) \right) \\
 &= W \log_2 \left(1 + a\theta(1-\theta) \left| (\sqrt{\rho} \hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho} \mathbf{e})^H \right. \right. \\
 &\quad \times \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \Big\| \|\mathbf{h}_{S,R}\|^4 \Big/ \left(b\theta \left| (\sqrt{\rho} \hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho} \mathbf{e})^H \right. \right. \\
 &\quad \times \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \Big\| \|\mathbf{h}_{S,R}\|^2 + (c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1) \Big) \Big) \quad (12) \\
 &= W \log_2 \left(1 + a\theta(1-\theta) (\rho \|\hat{\mathbf{h}}_{R,D}\|^2 + 2\sqrt{\rho(1-\rho)} \right. \\
 &\quad \times \mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) + (1-\rho) \|\mathbf{e} \hat{\mathbf{h}}_{R,D}^H\|^2 / \|\hat{\mathbf{h}}_{R,D}\|^2) \|\mathbf{h}_{S,R}\|^4 \\
 &\quad \Big/ \left(b\theta (\rho \|\hat{\mathbf{h}}_{R,D}\|^2 + 2\sqrt{\rho(1-\rho)} \mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) \right. \\
 &\quad \left. \left. + (1-\rho) \|\mathbf{e} \hat{\mathbf{h}}_{R,D}^H\|^2 / \|\hat{\mathbf{h}}_{R,D}\|^2) \|\mathbf{h}_{S,R}\|^2 + (c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1) \right) \right) \\
 &\approx W \log_2 \left(1 + a\theta(1-\theta) \rho \|\hat{\mathbf{h}}_{R,D}\|^2 \|\mathbf{h}_{S,R}\|^4 \right. \\
 &\quad \left. \Big/ (b\theta \rho \|\hat{\mathbf{h}}_{R,D}\|^2 \|\mathbf{h}_{S,R}\|^2 + c(1-\theta) \|\mathbf{h}_{S,R}\|^2 + 1) \right) \quad (13) \\
 &\approx W \log_2 \left(1 + \frac{a\theta(1-\theta) \rho N_R^3}{b\theta \rho N_R^2 + c(1-\theta) N_R + 1} \right), \quad (14)
 \end{aligned}$$

where W is a half of the spectral bandwidth, since a complete transmission requires two time slots. $\mathcal{R}(x)$ denotes the real part of x . $\mathbf{h}_{R,D}$ is replaced by $\sqrt{\rho} \hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho} \mathbf{e}$ in (12). (13) follows from the fact that $\rho \|\hat{\mathbf{h}}_{R,D}\|^2$ scales with the order $\mathcal{O}(\rho N_R)$ as $N_R \rightarrow \infty$ while $2\sqrt{\rho(1-\rho)} \mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) + (1-\rho) \|\mathbf{e} \hat{\mathbf{h}}_{R,D}^H\|^2 / \|\hat{\mathbf{h}}_{R,D}\|^2$ scales as the order $\mathcal{O}(1)$, which can be negligible. (14) holds true because of $\lim_{N_R \rightarrow \infty} \frac{\|\hat{\mathbf{h}}_{R,D}\|^2}{N_R} = 1$ and $\lim_{N_R \rightarrow \infty} \frac{\|\mathbf{h}_{S,R}\|^2}{N_R} = 1$, namely channel hardening [16]. Therefore, we get the Theorem 1.

APPENDIX B PROOF OF THEOREM 2

According to (10), for a given ε , we have

$$\begin{aligned}
 \varepsilon &= P_r(C_{SOC} > C_D - W \log_2(1 + \gamma_E)) \\
 &= P_r(\gamma_E > 2^{(C_D - C_{SOC})/W} - 1) \\
 &= 1 - F\left(2^{(C_D - C_{SOC})/W} - 1\right), \quad (15)
 \end{aligned}$$

where $F(x)$ is the cumulative distribution function (cdf) of γ_E . In order to derive the secrecy outage capacity, the key is to get the cdf of γ_E . Examining (9), due to channel hardening, we have

$$\gamma_E = \frac{e\theta(1-\theta)N_R^2 \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2}{f\theta N_R \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 + c(1-\theta)N_R + 1}. \quad (16)$$

Since $\hat{\mathbf{h}}_{R,D}/\|\hat{\mathbf{h}}_{R,D}\|$ is an isotropic unit vector and independent of $\mathbf{h}_{R,E}$, $\left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2$ is χ^2 distributed with 2 degrees of freedom. Let $y \sim \chi_2^2$, we can derive the cdf of γ_E as

$$F(x) = P_r \left(\frac{e\theta(1-\theta)N_R^2 y}{f\theta N_R y + c(1-\theta)N_R + 1} \leq x \right). \quad (17)$$

If $x < e(1-\theta)N_R/f$, then we have

$$\begin{aligned} F(x) &= P_r \left(y \leq \frac{(c(1-\theta)N_R + 1)x}{e\theta(1-\theta)N_R^2 - f\theta N_R x} \right) \\ &= 1 - \exp \left(-\frac{(c(1-\theta)N_R + 1)x}{e\theta(1-\theta)N_R^2 - f\theta N_R x} \right). \end{aligned} \quad (18)$$

Since $x \geq e(1-\theta)N_R/f$ is impossible when $x = 2^{(C_D - C_{SOC})/W} - 1$, we have

$$\varepsilon = \exp \left(-\frac{(c(1-\theta)N_R + 1)x}{e\theta(1-\theta)N_R^2 - f\theta N_R x} \right). \quad (19)$$

Equivalently, we have

$$\begin{aligned} C_{SOC} &= W \log_2 \left(1 + \frac{a\theta(1-\theta)\rho N_R^3}{b\theta\rho N_R^2 + c(1-\theta)N_R + 1} \right) \\ &\quad - W \log_2 \left(1 + \frac{e\theta(1-\theta)N_R^2 \ln \varepsilon}{f\theta N_R \ln \varepsilon - c(1-\theta)N_R - 1} \right). \end{aligned} \quad (20)$$

Hence, we get the Theorem 2.

APPENDIX C PROOF OF THEOREM 3

For the secrecy outage capacity in (20), if the transmit power P_S is sufficiently large, it can be approximated as

$$\begin{aligned} C_{SOC} &\approx W \log_2 \left(\frac{a\theta(1-\theta)\rho N_R^3}{b\theta\rho N_R^2 + c(1-\theta)N_R} \right) \\ &\quad - W \log_2 \left(\frac{e\theta(1-\theta)N_R^2 \ln \varepsilon}{f\theta N_R \ln \varepsilon - c(1-\theta)N_R} \right) \end{aligned} \quad (21)$$

$$\begin{aligned} &= W \log_2 \left(\frac{\eta P_S \alpha_{S,R} \alpha_{R,D} \theta (1-\theta) \rho N_R^2}{\eta \alpha_{R,D} \theta \rho N_R + 1 - \theta} \right) \\ &\quad - W \log_2 \left(\frac{\eta P_S \theta \alpha_{R,E} N_R \alpha_{S,R} (1-\theta) \ln \varepsilon}{\eta \theta \alpha_{R,E} \ln \varepsilon - (1-\theta)} \right) \\ &= W \log_2 \left(\frac{\alpha_{R,D} N_R (\eta \theta \alpha_{R,E} \ln \varepsilon - (1-\theta))}{(\eta \alpha_{R,D} \theta N_R + (1-\theta)) \alpha_{R,E} \ln \varepsilon} \right), \end{aligned} \quad (22)$$

where (21) holds true since the constant “1” is negligible when P_S is large enough. It is found that the secrecy outage capacity in this case is independent of transmit power P_S . Thus, we prove the Theorem 3.

REFERENCES

- [1] F. Zhang, S. A. Hackworth, X. Liu, H. Chen, R. J. Sclabassi, and M. Sun, “Wireless energy transfer platform for medical sensor and implantable devices,” in *Proc. IEEE EMBS 31st Annual Int. Conf.*, pp. 1045-1048, Sep. 2009.
- [2] P. Grover, and A. Sahai, “Shannon meets Tesla: wireless information and power transfer,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2363-2367, June 2010.
- [3] K. Huang, and E. G. Larsson, “Simultaneous information and power transfer for broadband wireless systems,” *IEEE Trans. Signal Process.*, vol. 61, no. 23, pp. 5972-5986, Dec. 2013.
- [4] R. Zhang, and C. K. Ho, “MIMO broadcasting for simultaneous wireless information and power transfer,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 3543-3553, May 2013.
- [5] Z. Xiang, and M. Tao, “Robust beamforming for wireless information and power transmission,” *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 372-375, Aug. 2012.
- [6] X. Chen, C. Yuen, and Z. Zhang, “Wireless energy and information transfer tradeoff for limited feedback multi-antenna systems with energy beamforming,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 407-412, Jan. 2014.
- [7] X. Chen, X. Wang, and X. Chen, “Energy-efficient optimization for wireless information and power transfer in large-scale MIMO systems employing energy beamforming,” *IEEE Wireless Commun. Lett.*, vol. 2, no. 6, pp. 667-670, Dec. 2013.
- [8] D. S. Michalopoulos, H. A. Suraweera, and R. Schober, “Relay selection for simultaneous information transfer and wireless energy transfer: a tradeoff perspective,” [online]: <http://arxiv.org/abs/1303.1647v1>.
- [9] Z. Chen, B. Wang, B. Xia, and H. Liu, “Wireless information and power transfer in two-way amplify-and-forward relaying channels,” [online]: <http://arxiv.org/abs/1307.7447v1>.
- [10] P. K. Gopala, L. Lai, and H. El. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.
- [11] X. Chen, L. Lei, H. Zhang, and C. Yuen, “On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI,” in *Proc. IEEE ICC*, pp. 1-6, Jun. 2014.
- [12] L. Liu, R. Zhang, and K. C. Chua, “Secrecy wireless information and power transfer with MISO beamforming,” *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850-1863, Apr. 2014.
- [13] D. W. K. Ng, E. S. Lo, and R. Schober, “Robust beamforming for secure communication in systems with wireless information and power transfer,” [online]: <http://arxiv.org/abs/1311.2507v1>.
- [14] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physical-layer security in cooperative wireless networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.
- [15] D. S. W. Hui, and V. K. N. Lau, “Design and analysis of delay-sensitive cross-layer OFDMA systems with outdated CSIT,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3484-3491, Jul. 2009.
- [16] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, “Multiple-antenna channel hardening and its implications for rate-feedback and scheduling,” *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893-1909, Sept. 2004.